

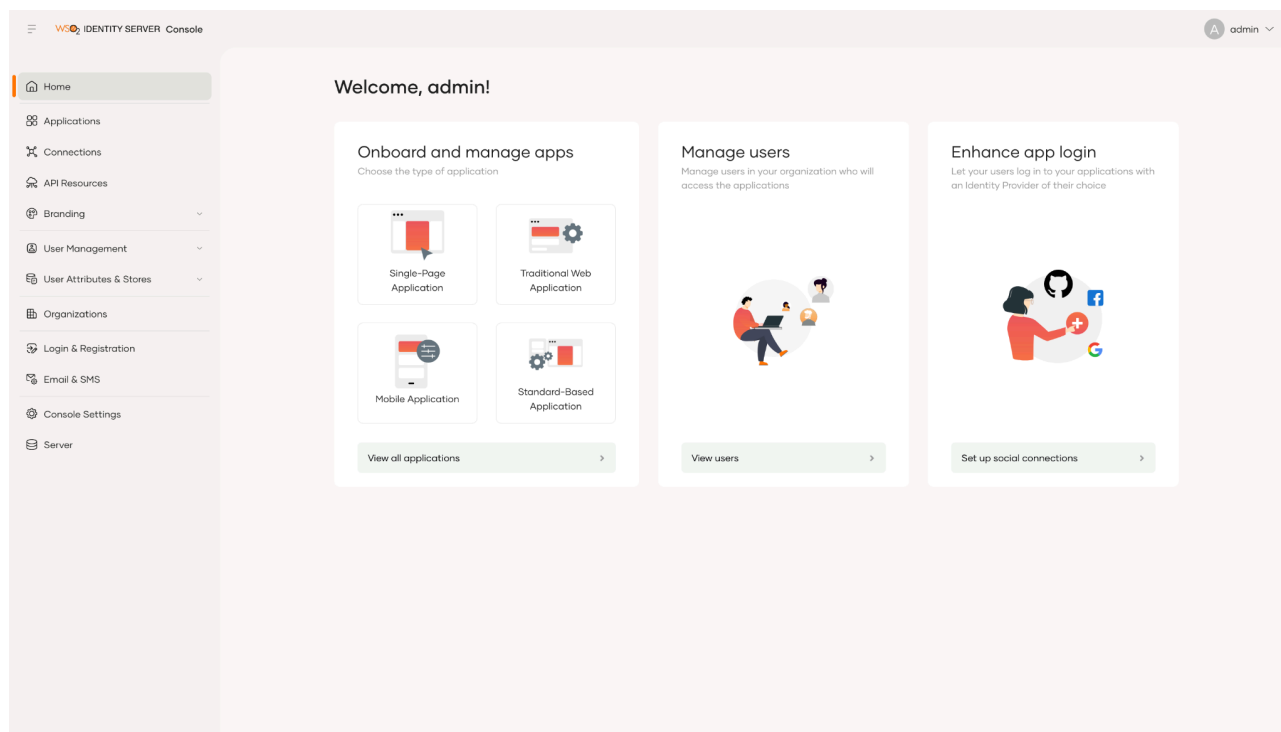
# User, Group and Role Management

## Introduction

In this tutorial, we are going to try out the User, Group and Role Management in WS02 Identity Server. This topic involves,

1. managing users, groups, roles.
2. managing permissions associated with roles and groups.
3. assigning users into groups and roles.

These user management tasks can be performed in various ways including using the Console app, using APIs and using My Account.



## Lab 01: User Management via Console

Let's create a user and assign the user to a group. And then create a role and assign the role to the group. This way, users will have permissions associated with the roles assigned to the group.

### Access Console

To access the Wso2 Identity Server Console, follow these steps:

1. Download the latest version of WSO2 Identity Server from [the web site](#).
2. Please verify that all the [system requirements](#) are satisfied.
  - Java version should 11 or 17
3. Navigate to <IS\_HOME>/bin and start the server by executing either of the following,  
  
`./wso2server.sh` (Ubuntu , Mac) or `./wso2server.bat` run (Windows)
4. Log in to the [Console App \(https://localhost:9443/console\)](https://localhost:9443/console), and enter **admin** as both the username and the password.



WSO<sub>2</sub> IDENTITY SERVER

Sign In

Username

 Enter your username

Password


 Enter your password 

Forgot [username](#) or [password](#) ?

☐ Remember me on this computer

Sign In

© 2024 WSO2 LLC.

[Privacy Policy](#) [Terms of Service](#)  [English - United States](#) ▼

## Add New Users

To add a new user, follow these steps:

1. Expand the **User Management** menu item, click on **Users**.
2. On the **Users** page, click **Add User** and select **Single User** from the dropdown.
3. In the opened up wizard,
  - Keep **Primary** as the user store.
  - Add the below configuration to the respective fields.
    - Username: **john**
    - Email: [john@wso2.com](mailto:john@wso2.com)
    - First Name: **John**
    - Last Name: **Doe**
  - When you scroll down a bit, you will see 2 options as the method to set the user password. For the simplicity of the guide, select **Set a password for the user** option.
    - When **Invite the user to set their own password** option is selected, an email will be sent to the configured email address and the user will have to goto the link to get to the password setting page. There, the user can add the preferred password.
4. As we selected **Set a password for the user** option add the below password as the user password.
  - Password: **John@1234**

**Create User**  
Follow the steps to create a new user.

Basic Details — User Groups — Invitation

Select user store \*  
Primary

Username \*  
john

Email \*  
john@wso2.com

First Name \*  
John

Last Name \*  
Doe

Select the method to set the user password  
☐ Invite the user to set their own password

Cancel Next →

5. Click **Next**.
6. As we have not added any groups yet, skip group selection and Click **Save & Continue**.
7. Click **Close**.

## Add New Groups

Group is a collection of users who are managed as a single unit within the organization to streamline assigning permissions and roles.

To add a new groups, follow these steps:

1. Expand the **User Management** menu item, click **Groups**.
2. On the **Groups** page, click **New Group**.
3. Enter **Managers** as the group name.
4. From the list of users, select **john** as a member of the Managers group.
5. Click **Next**.

**Create Group**  
Create new group and add users to the group.

**Basic Details** | Assign Roles

User Store \*  
Primary

Group Name \*  
Managers

A name for the group. Can contain between 3 to 30 alphanumeric characters, dashes (-), and underscores (\_).

**Add Users**  
Select users to add them to the user group.

Search users

☐ admin

Cancel | Next →

6. As we have not created any roles yet, skip role selection and Click **Finish**.

## Add New User Role

Role represents a set of permissions and responsibilities assigned to a user or group of users within an application, or organization.

### Organization Role

Organization roles are defined in the organization level and can be used in the application level when multiple applications use the same access privileges.

To add a new user role, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.

The screenshot shows the WSO2 Identity Server Console interface. On the left is a sidebar menu with items: Home, Applications, Connections, API Resources, Branding, User Management (expanded), Users, Groups, Roles (selected), User Attributes & Stores, Organizations, Login & Registration, Email & SMS, Console Settings, and Server. The main content area is titled 'Roles' and includes a subtitle 'Create and manage roles, assign permissions for roles.' and a '+ New Role' button. Below this is a search bar 'Search by role name' and a 'Filter By' dropdown. A table lists existing roles:

Role	Audience	
S system	organization	
E everyone	organization	
A admin	organization	

At the bottom of the table area, there is an 'Items per page' dropdown set to '10' and 'Previous' and 'Next' navigation buttons.

2. On the **Roles** page, click **New Role**.
3. Enter **Manager** as the role name.

#### 4. Select **Organization** as the role audience.

WSO<sub>2</sub> IDENTITY SERVER Console

admin

Go back

### Create Role

Create a new role in the system.

#### 1 Basic Details

Role Name \*

Manager

Select the role audience \*

☐ Application

☒ Organization

Set the audience of the role. Note that audience of the role cannot be changed.

When the role audience is organization, you can associate the role with an application which allows organization audience roles.

Next

#### 2 Permission Selection

5. Click **Next** to goto the **Permission Selection** section.
6. Choose relevant scope from the drop down given. (To maintain the simplicity of this section, let's skip the step)
7. Click **Finish**.
8. On the Role page, goto **Groups** tab and click on **Assign Groups** to add groups.
9. From the dropdown, select **Managers** group.
10. Click **Update**.

## Application Role

These types of roles are tailored to the specific requirements of an application. Further details about application roles such as usage will be discussed in **12. API Authorization** tutorial.










## Update Existing User Role

To update the Manager role that you previously added, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.
2. On the **Roles** page, the **Manager** role is displayed in the list of roles.
3. Click on the **Edit** button.

The screenshot shows the WSO2 Identity Server Console interface. On the left, a sidebar menu lists various management options, with 'Roles' selected under the 'User Management' section. The main panel is titled 'Roles' and includes a search bar and a 'Filter By' dropdown. Below this is a table listing roles:

Role	Audience	Actions
M Manager	organization	 
S system	organization	 
E everyone	organization	 
A admin	organization	

At the bottom of the table, there is a pagination control showing 'Items per page' set to 10, and 'Previous' and 'Next' buttons.

4. Enter a new name in the **Role name** area, and click **Update**.

The screenshot displays the WSO2 Identity Server Console interface. On the left is a sidebar menu with options: Home, Applications, Connections, API Resources, Branding, User Management (expanded), Users, Groups, Roles (selected), User Attributes & Stores, Organizations, Login & Registration, Email & SMS, Console Settings, and Server. The main content area is titled 'Manager' and includes a 'Go back to roles' link. Below the title, it states 'Can be used within the organization: Super'. There are tabs for 'Basics' (active), 'Permissions', 'Groups', 'Users', and 'Connected Apps'. The 'Basics' tab contains a 'Role Name' input field with the value 'ManagerR' and an 'Update' button. Below this is a 'Danger Zone' section with a 'Delete role' warning: 'Once you delete the role, it cannot be recovered.' and a 'Delete Role' button.

## Delete User Roles

To delete a role, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.
2. Click on the **bin** icon of the relevant role to **Delete role**.

WSO<sub>2</sub> IDENTITY SERVER Console

admin

Home

Applications

Connections

API Resources

Branding

User Management

Users

Groups

Roles

User Attributes & Stores

Organizations

Login & Registration

Email & SMS

Console Settings

Server

Roles

Create and manage roles, assign permissions for roles.

+ New Role

Search by role name

Filter By

Role	Audience	
M Manager	organization	<div><div></div><div></div></div>
S system	organization	<div><div></div><div></div></div>
E everyone	organization	<div><div></div><div></div></div>
A admin	organization	<div><div></div></div>

Items per page 10

Previous

Next

## Assign Permissions to a User Role

To assign permissions to a specific user role, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.
2. On the **Roles page**, click on the **Edit** button of the **Manager** role displayed in the list of roles.
3. Click on the **Permissions** tab to add a permission.
4. When you expand the drop down of **Select API Resource**, the available API resources are listed as options. By selecting the API resources you will be giving the role to have access to the selected API resources.
5. Select the **SCIM2 Roles API** under **Management APIs** as the **API resource**.
6. After selecting an API Resource you need to select the **level of permissions(scopes)** you want to have for the selected API Resource. ex: view, edit, update, delete
7. Select **View Role and Create Role** as the scope.
8. Click **Update**.

## Try It

To verify whether the users, role, and group you defined are correctly updated, follow these steps:

1. Expand User Management menu Item and select Groups.
2. Select **Managers** Group.
3. Goto the Users tab.
  - You should see **john** listed as a user.
4. Goto the Roles tab.
  - You should see **Manager** listed as a role.

## Lab 02: User Self-Registration via My Account

To learn how a user can self-register via My Account, follow these steps:

1. To enable self user registration in your organization, follow these sub-steps:
  - a. On the WSO2 Identity Server Console, go to **Login & Registration > User Onboarding > Self Registration**.

The screenshot displays the WSO2 Identity Server Console interface. On the left is a sidebar menu with options: Home, Applications, Connections, API Resources, Branding, User Management, User Attributes & Stores, Organizations, Login & Registration (highlighted), Email & SMS, Console Settings, and Server. The main content area is titled 'Self Registration' and includes a 'Go back to login & registration' link. Below the title is a description: 'When self registration is enabled, users can register via the **Create an account** link on the application's login page. This creates a new account in the organization.' A toggle switch for 'Self Registration' is currently in the 'Disabled' position. Below this, there are several configuration options: 'Account verification' is checked, with a note 'An email is sent to the self-registered user requesting account verification.'; 'Account verification link expiry time' is set to '1440 mins'; 'Activate account immediately' is unchecked, with a blue callout box stating 'If selected, the new account is activated immediately after registration without waiting for account confirmation.'; 'Enable auto login' is unchecked, with a note 'If selected, the user will be automatically logged in after registration.'; and 'Send sign up confirmation email' is unchecked.

- b. Toggle the switch to enable self-registration.
    - c. Leave the other configurations unchanged.
    - d. Click **Update** to save the changes.

2. To send the sign up confirmation email, configure the email server to send emails by following the below steps.
  - a. Open the `deployment.toml` file in the `<IS_HOME>/repository/conf` path.
  - b. Specify values for the `from_address`, `username`, and `password` parameters in the `[output_adapter.email]` section as shown in the extract below:

```
[output_adapter.email]
from_address="<email>"
username="<email>"
password="<password>"
hostname="smtp.gmail.com"
port=587
enable_start_tls=true
enable_authentication=true
```

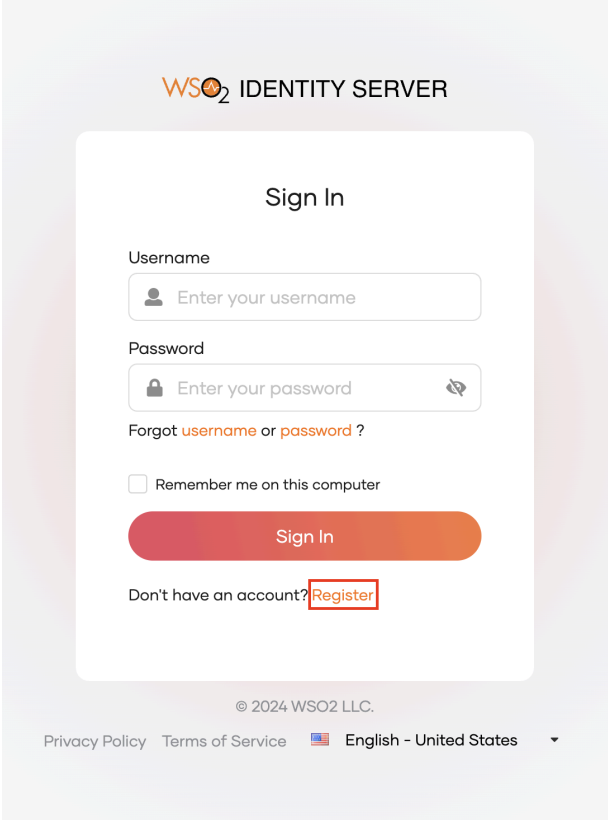
(if you are using a gmail account as the sender, create an [App password](#) and use that as the password. If your password contains invalid characters such as ">" , "<" and "&", enter the password as "<![CDATA[xxxx]]>")

- c. Restart the WSO2 Identity Server.

## Try It

To verify whether you have successfully enabled self-registration, follow these sub-steps:

1. Access [My Account](#) and click **Register**.

The image shows a screenshot of the WSO2 Identity Server 'Sign In' page. The page has a light gray background. At the top, the WSO2 logo is followed by the text 'IDENTITY SERVER'. Below this is a white rounded rectangle containing the 'Sign In' form. The form has two input fields: 'Username' with a user icon and 'Password' with a lock icon. Below the password field is a link 'Forgot username or password?'. There is a checkbox for 'Remember me on this computer'. A large orange 'Sign In' button is centered. At the bottom of the form, it says 'Don't have an account?' followed by a red-outlined 'Register' button. The footer of the page includes '© 2024 WSO2 LLC.', 'Privacy Policy', 'Terms of Service', and a language selector set to 'English - United States'.

2. Click on **Continue with email**.
3. Specify values for the user account.



## WSO2 IDENTITY SERVER

### Sign Up

Username \*

Email \*

Password \*

- Must be between 8 and 30 characters
- At least 1 uppercase and 1 lowercase character(s)
- At least 1 number(s)
- At least 1 special character(s)

First Name \*

Last Name \*

Country

Mobile

Sign Up

Already have an account? [Sign in](#)

© 2024 WSO2 LLC.

[Privacy Policy](#)

English - United States

4. Click **Sign Up**.
5. Check the inbox of the registered email account. You must have received an email to activate the account created. Click on that link to confirm the account.
6. Go to [My account](#) and log in using created users credentials. You should be able to log in.

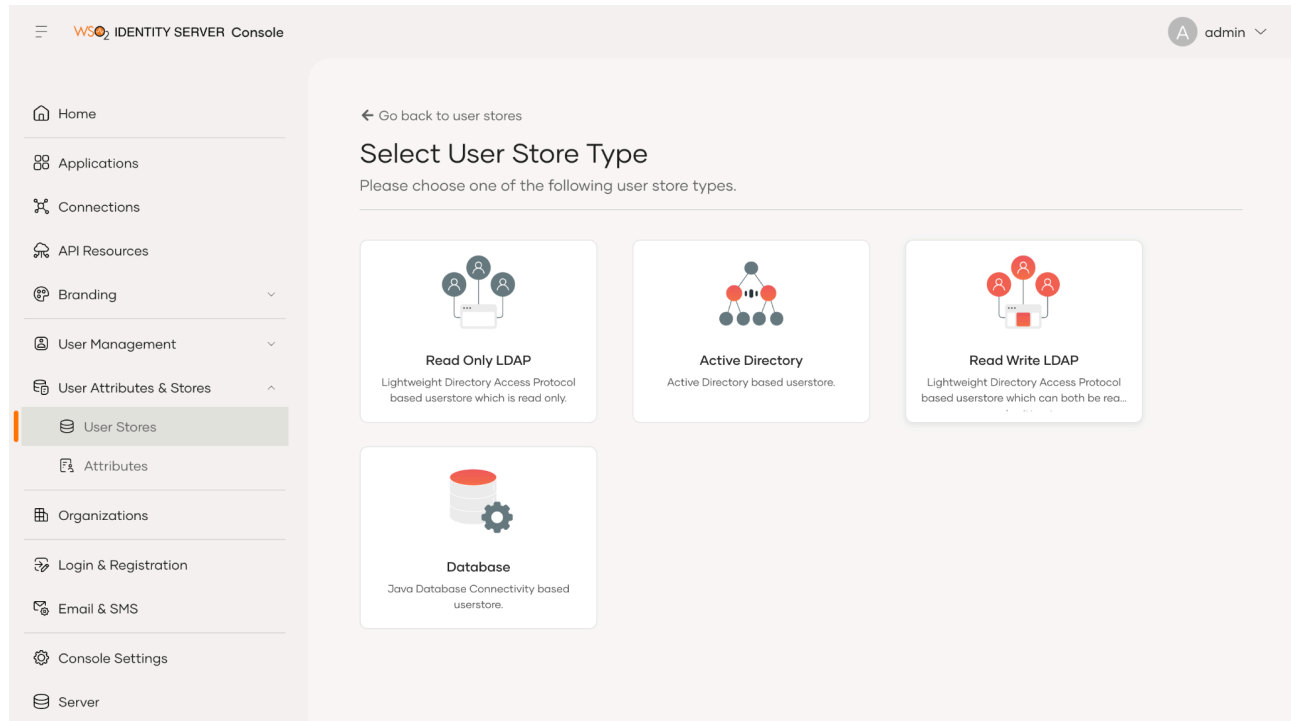
## Lab 03: Setting up a Secondary User Store

In this lab, you will set up the Mysql JDBC Database as a secondary user store in WSO2 IAM and connect a user to it.

### Setting Up

To set up the MySQL-based secondary user store, follow these steps:

1. First Create a Mysql database.
2. Execute `<IS_HOME>/dbscripts/mysql.sql` against the created database to create the database tables.
3. Download the [Mysql driver](#)(mysql connector) and extract the zip find to the `mysql-connector-j-<version>.jar` inside the extracted folder.
4. Locate the jar under `<IS_HOME>/repository/components/lib` folder.
5. Restart the WSO2 Identity Server.
6. On the WSO2 Identity Server Console, go to **User Attributes & Stores > User Stores**.
7. Click **New User Store** and select the user store type.



8. Select Database as the option.

9. Enter the below mentioned values for the mandatory fields.

a. **Name:** ABCDEmployees

b. **Connection URL:**

`jdbc:mysql://localhost:3306/{Database_Name}?useSSL=false&allowPublicKeyRetrieval=true`

c. **Connection Name:** Username of the DB User

d. **Connection Password:** Password of the DB User

e. **Driver Name:** `com.mysql.cj.jdbc.Driver`

10. To test the connection click on **Test Connection** and verify.

Add Database User Store

General User Group Summary

Name \*

Enter a name

Description

Enter a description

☒ Enabled

☐ Read-only

Connection URL \*

Enter a Connection URL

Connection Name \*

Enter a Connection Name

Connection Password \*

Enter a Connection Password

Cancel Next →

11. Click **Next**.
12. Click **Next** from the User section.
13. Click **Next** from the Group section.
14. Click **Finish**.
15. Refresh the page after a few seconds to check the status. If the new user store is successfully added, it will appear in the user stores page.

## Let's try adding a user to the secondary user store

1. On the WSO2 Identity Server Console, go to **User Management > Users**.
2. Click on **Add User** and select **Single User**.
3. In the create user wizard, when you expand the **Select user store** dropdown, one should be able to see the user store created.

Create User

Follow the steps to create a new user.

Basic Details User Groups Invitation

Select user store \*

Primary

Primary

ABCEmployees

Email \*

Enter the email address

First Name \*

Enter the first name

Last Name \*

Enter the last name

Select the method to set the user password

Cancel Next →

4. Select the created **ABCEmployees** secondary user store and fill the relevant information of the user.
5. Now a user is added to the secondary user store.
6. Query the UM\_USER table in the MySQL database. You will see that the user is created.

```
SELECT * FROM UM_USER;
```